CLAIMS

1. A quantum key distribution method employed on a quantum cryptosystem including a first communication apparatus that transmits photons onto a quantum communication path and a second communication apparatus that measures the photons, comprising:

a check matrix creation step of each of the first communication apparatus and the second communication apparatus creating the same parity check matrices $H(n \times k)$;

a random number generation step of the first communication apparatus generating a random number sequence (transmission data) and randomly determining a predetermined transmission code (base) by the first communication apparatus, and the second communication apparatus randomly determining a predetermined reception code (base);

a photon transmission step of the first communication apparatus transmitting a photon onto the quantum communication path while the photon is in a quantum state specified by a combination of the transmission data and the transmission code;

a photon reception step of the second communication apparatus measuring the photon transmitted on the quantum communication path to obtain reception data specified by the combination of the reception code and measurement result;

a data deletion step of each of the first communication apparatus and the second communication apparatus deciding whether the measuring has been performed with an appropriate measuring

apparatus, saving the reception data of n bits if the measuring has been performed with the appropriate measuring apparatus and transmission data that corresponds to the reception data, and discarding other pieces of the data;

an error correction information notification step of the first communication apparatus notifying the second communication apparatus through a public communication path of error correction information of k bits based on the parity check matrix H and the transmission data of n bits;

an error correction step of the second communication apparatus correcting the error of the reception data based on the parity check matrix H, the reception data of n bits, and the error correction information; and

a cryptographic key creation step of each of the first communication apparatus and the second communication apparatus discarding a part (k) of pieces of the common information (n) after correction according to public error correction information, creating a cryptographic key using information that has remained after discarding, and setting the cryptographic key as a common key which is shared between apparatuses.

2. The quantum key distribution method according to claim 1, wherein the check matrix creation step includes

weight searching step of using finite affine geometry as a basic matrix and searching optimum row and column weight distributions of

the parity check matrix by performing optimization of Gaussian approximation,

dividing step of dividing randomly the row and column weights of the finite affine geometry based on the optimum weight distribution by a predetermined procedure, and creating the parity check matrix H of a low-density parity check code in which both the row and column weights or one of the row and column weights is not uniform.

3. The quantum key distribution method according to claim 1, wherein the check matrix creation step includes creating an inverse matrix $G^{-1}(n\times(n-k))$, which satisfies $G^{-1}\cdot G=I$ (unit matrix), from a creation matrix $G((n-k)\times n)$ satisfying "HG=0," and

the cryptographic key creation step includes discarding a part (k) of pieces of the common information (n) by the inverse matrix G^{-1}.

4. The quantum key distribution method according to claim 3, wherein the cryptographic key creation step includes

one of the communication apparatus, out of the first communication apparatus and the second communication apparatus, creating a nonsingular random matrix $R((n-k)\times(n-k))$ to act on the cryptographic key after discarding a part (k) of pieces of the common information (n) and informing the nonsingular random matrix R to other one of the communication apparatuses through a public communication path,

the first communication apparatus and the second

communication apparatus using the nonsingular random matrix R to create the cryptographic key.

5. The quantum key distribution method according to claim 1, wherein the check matrix creation step includes creating a mapping F to map an n-dimensional vector to an m-dimensional vector ($m \leq n-k$), the mapping F being one in which the number of elements of a reverse image $(F \cdot G)^{-1}(v)$ in a composition mapping $F \cdot G$ of the mapping F and the creation matrix G satisfying "HG=0" is independent of an arbitrary m-dimensional vector v and is constant(2^{n-k-m}), and

the cryptographic key creation step includes discarding a part of pieces of the common information (n) by the mapping F.

6. The quantum key distribution method according to claim 5, wherein the cryptographic key creation step includes

one of the communication apparatus, out of the first communication apparatus and the second communication apparatus, creating a nonsingular random matrix $R((n-k)\times(n-k))$ to act on the cryptographic key after discarding a part (k) of pieces of the common information (n) and informing the nonsingular random matrix R to other one of the communication apparatuses through a public communication path,

the first communication apparatus and the second communication apparatus using the nonsingular random matrix R to create the cryptographic key.

7. The quantum key distribution method according to claim 2, wherein the cryptographic key creation step includes performing random permutation to the column of the parity check matrix H, selecting specific "1" in the first column of finite affine geometry $AG(2,2^S)$ of a creation element of the parity check matrix H, exchanges a position of "1" through a public communication path, specifying the position (column) after the division corresponding to "1" from the parity check matrix after the random permutation and the position (column) after the division corresponding to "1" in each cyclically shifted column, and discarding a part (k) of pieces of the common information (n) corresponding to the specified position (column).

8. The quantum key distribution method according to claim 7, wherein the cryptographic key creation step includes

one of the communication apparatus, out of the first communication apparatus and the second communication apparatus, creating a nonsingular random matrix $R((n-k)\times(n-k))$ to act on the cryptographic key after discarding a part (k) of pieces of the common information (n) and informing the nonsingular random matrix R to other one of the communication apparatuses through a public communication path,

the first communication apparatus and the second communication apparatus using the nonsingular random matrix R to create the cryptographic key.

9. A communication apparatus on transmission side that transmits photons onto a quantum communication path, comprising:

a check matrix creation unit that creates a parity check matrix H(n×k) identical to a communication apparatus on reception side;

a transmission unit that generates a random number sequence (transmission data), randomly determines a predetermined transmission code (base), transmits the photon onto the quantum communication path while the photon is in a quantum state specified by a combination of the transmission data and the transmission code, decides whether the measuring has been performed with an appropriate measuring apparatus in the communication apparatus on the reception side, saves the transmission data of n bits if the measuring has been performed with the appropriate measuring apparatus, and discards other pieces of the transmission data;

an error correction information notifying unit that notifies the communication apparatus on the reception side of error correction information of k bits based on the parity check matrix H and the transmission data of n bits through a public communication path; and

a cryptographic key creation unit that discards a part (k) of pieces of the common information (n) after error correction according to public error correction information, creates a cryptographic key using information that has remained after discarding, and sets the cryptographic key as a common key which is shared with the communication apparatus on the reception side.

10. The communication apparatus according to claim 9, wherein the check matrix creation unit uses finite affine geometry as a basic matrix, searches optimum row and column weight distributions of the parity check matrix by performing optimization of Gaussian approximation,

divides randomly the row and column weights of the finite affine geometry based on the optimum weight distribution by a predetermined procedure, and

creates the parity check matrix H of a low-density parity check code in which both the row and column weights or one of the row and column weights is not uniform.

11. The communication apparatus according to claim 9, wherein the check matrix creation unit further creates an inverse matrix $G^{-1}(n\times(n-k))$, which satisfies $G^{-1}\cdot G=I$ (unit matrix), from a creation matrix $G((n-k)\times n)$ satisfying "HG=0," and

the cryptographic key creation unit discards a part (k) of pieces of the common information (n) by the inverse matrix G^{-1}.

12. The communication apparatus according to claim 11, wherein the cryptographic key creation unit uses a nonsingular random matrix $R((n-k)\times(n-k))$ as the cryptographic key after discarding a part (k) of pieces of the common information (n).

13. The communication apparatus according to claim 9, wherein the

check matrix creation unit further creates a mapping F to map an n-dimensional vector to an m-dimensional vector ($m \leq n-k$), the mapping F being one in which the number of elements of a reverse image $(F \cdot G)^{-1}(v)$ in a composition mapping $F \cdot G$ of the mapping F and the creation matrix G satisfying "HG=0" is independent of an arbitrary m-dimensional vector v and is constant(2^{n-k-m}), and

the cryptographic key creation unit discards a part of pieces of the common information (n) by the mapping F.

14. The communication apparatus according to claim 13, wherein the cryptographic key creation unit uses a nonsingular random matrix $R((n-k)\times(n-k))$ as the cryptographic key after discarding a part (k) of pieces of the common information (n).

15. The communication apparatus according to claim 10, wherein the cryptographic key creation unit performs random permutation to the column of the parity check matrix H, selects specific "1" in the first column of finite affine geometry $AG(2,2^S)$ of a creation element of the parity check matrix H, exchanges a position of "1" through a public communication path, specifies the position (column) after the division corresponding to "1" from the parity check matrix after the random permutation and the position (column) after the division corresponding to "1" in each cyclically shifted column, and discards a part (k) of pieces of the common information (n) corresponding to the specified position (column).

16. The communication apparatus according to claim 15, wherein the cryptographic key creation unit uses a nonsingular random matrix R((n-k)×(n-k)) as the cryptographic key after discarding a part (k) of pieces of the common information (n).

17. A communication apparatus on reception side that measures photons on a quantum communication path, comprising:

a check matrix creation unit that creates a parity check matrix H(n×k) identical to a communication apparatus on transmission side;

a receiving unit that randomly determines a predetermined reception code (base), measures the photons on the quantum communication path, reproduces reception data specified by a combination of the reception code and measurement result, decides whether the measuring has been performed with an appropriate measuring apparatus, saves the reception data of n bits if the measuring has been performed with the appropriate measuring apparatus, and discards other pieces of the reception data;

an error correction unit that corrects the error of reception data based on error correction information of k bits received through a public communication path, the parity check matrix H, and the reception data of n bits; and

a cryptographic key creation unit that discards a part (k) of pieces of the common information (n) after error correction according to public error correction information, creates a cryptographic key using

information that has remained after discarding, and sets the cryptographic key as a common key which is shared with the communication apparatus on the transmission side.

18. The communication apparatus according to claim 17, wherein the check matrix creation unit uses finite affine geometry as a basic matrix, searches optimum row and column weight distributions of the parity check matrix by performing optimization of Gaussian approximation,

divides randomly the row and column weights of the finite affine geometry based on the optimum weight distribution by a predetermined procedure, and

creates the parity check matrix H of a low-density parity check code in which both the row and column weights or one of the row and column weights is not uniform.

19. The communication apparatus according to claim 17, wherein the check matrix creation unit further creates an inverse matrix $G^{-1}(n\times(n-k))$, which satisfies $G^{-1}\cdot G=I$ (unit matrix), from a creation matrix $G((n-k)\times n)$ satisfying "HG=0," and

the cryptographic key creation unit discards a part (k) of pieces of the common information (n) by the inverse matrix G^{-1}.

20. The communication apparatus according to claim 19, wherein the cryptographic key creation unit uses a nonsingular random matrix

R((n-k)×(n-k)) as the cryptographic key after discarding a part (k) of pieces of the common information (n).

21. The communication apparatus according to claim 17, wherein the check matrix creation unit further creates a mapping F to map an n-dimensional vector to an m-dimensional vector ($m \leq n-k$), the mapping F being one in which the number of elements of a reverse image $(F \cdot G)^{-1}(v)$ in a composition mapping $F \cdot G$ of the mapping F and the creation matrix G satisfying "HG=0" is independent of an arbitrary m-dimensional vector v and is constant(2^{n-k-m}), and

the cryptographic key creation unit discards a part of pieces of the common information (n) by the mapping F.

22. The communication apparatus according to claim 21, wherein the cryptographic key creation unit uses a nonsingular random matrix R((n-k)×(n-k)) as the cryptographic key after discarding a part (k) of pieces of the common information (n).

23. The communication apparatus according to claim 18, wherein the cryptographic key creation unit performs random permutation to the column of the parity check matrix H, selects specific "1" in the first column of finite affine geometry $AG(2,2^S)$ of a creation element of the parity check matrix H, exchanges a position of "1" through a public communication path, specifies the position (column) after the division corresponding to "1" from the parity check matrix after the random

permutation and the position (column) after the division corresponding to "1" in each cyclically shifted column, and discards a part (k) of pieces of the common information (n) corresponding to the specified position (column).

24. The communication apparatus according to claim 23, wherein the cryptographic key creation unit uses a nonsingular random matrix R((n-k)×(n-k)) as the cryptographic key after discarding a part (k) of pieces of the common information (n).